P24836.CL1

WHAT IS CLAIMED:

1. A method for providing secure communications through a communications network comprising ATM channels and TDM channels, the communications network including at least one closed user group of network elements configured to communicate with only other network elements in the closed user group, the method comprising:

receiving a connection setup request at an ingress ATM switch, via a UNI attached to the ATM switch, in response to a call initiated through a TDM channel, the UNI interfacing a first network element of the closed user group with the ATM switch;

verifying that an ATM End System Address (AESA) contained in calling party information of the connection setup request is consistent with the attached UNI; and

establishing a connection with at least a second network element of the closed user group through an egress ATM switch in the communications network when the AESA is consistent with the attached UNI.

2. The method for providing secure communications through the communications network, according to claim 1, further comprising:

denying access to the second network element of the closed user group when the AESA is not consistent with the attached UNI.

3. The method for providing secure communications through the communications network, according to claim 2, further comprising:

sending an alarm to an ATM element management system when the AESA is not consistent with the attached UNI.

4. The method for providing secure communications through the communications network, according to claim 1, in which the attached UNI comprises a physical port/UNI.

5. The method for providing secure communications through the communications network, according to claim 1, in which the attached UNI comprises a virtual UNI.

6. The method for providing secure communications through the communications network, according to claim 1, in which verifying the AESA comprises comparing a network prefix of the AESA to a network prefix previously assigned to the UNI.

7. The method for providing secure communications through the communications network, according to claim 1, further comprising:

establishing a membership list at an ATM element management system identifying each network element that is part of the closed user group; and

verifying that each of the first network element and the second network element belongs to the closed user group using the membership list, prior to establishing the connection.

8. The method for providing secure communications through the communications network, according to claim 1, in which the first network element and the second network

9. The method for providing secure communications through the communications network, according to claim 1, in which the connection comprises a switched virtual circuit connection.

10. A system for enforcing switched virtual circuit (SVC) access restrictions across an Asynchronous Transfer Mode (ATM) distributed virtual tandem switching system based on closed user groups of network elements in a communications network, the system comprising:

a plurality of trunk interworking function (T-IWF) devices in the communications network, configured to convert between voice streams from TDM communications channels to cell streams from ATM communications channels, a first one of the plurality of T-IWF devices receiving a call via at least one TDM communications channel from an end office;

a centralized control and signaling interworking function (CS-IWF) device that receives narrowband signaling data relating to routing the call, the CS-IWF device converting the narrowband signaling data to broadband signaling data to control the call through an ATM switching network and determining that the call is directed to a second one of the plurality of T-IWF devices, the plurality of T-IWF devices and the CS-IWF device being in a previously established closed user group; and

an ATM switch in the ATM switching network that receives a request from one of the CS-IWF device and the T-IWF devices to establish an SVC connection of the call over the ATM switching network;

wherein the ATM switch establishes the SVC connection over the ATM switching network, enabling broadband communication between the first T-IWF device and the second T-IWF device, when the CS-IWF device, the first T-IWF device and the second T-IWF device are determined to be in the closed user group; and

wherein the ATM switch does not establish the SVC connection over the ATM switching network when at least one of the CS-IWF device, the first T-IWF device and the second T-IWF device is determined not to be in the closed user group.

11. The system for enforcing SVC access restrictions according to claim 10, further comprising:

an ATM element management system that stores a list of network elements in the closed user group, including the CS-IWF device and the plurality of T-IWF devices, the determination of whether the CS-IWF device, the first T-IWF device and the second T-IWF device are in the closed user group being based on the list of network elements.

12. The system for enforcing SVC access restrictions according to claim 11, in which the ATM switch verifies that an ATM End System Address (AESA) contained in calling party information in the request from the CS-IWF device is consistent with a user-to-network

interface between the first T-IWF device and the ATM switch, the ATM switch rejecting the request to establish the SVC connection over the ATM switching network when the AESA is not consistent with the UNI.

13. The system for enforcing SVC access restrictions according to claim 12, in which the ATM switch sends an alarm to the ATM element management system when the AESA is not consistent with the UNI.

14. The system for enforcing SVC access restrictions according to claim 12, in which the UNI comprises a physical port/UNI.

15. The system for enforcing SVC access restrictions according to claim 12, in which the UNI comprises a virtual UNI.

16. A secure Asynchronous Transfer Mode (ATM) distributed virtual tandem switching system comprising:

a signaling transfer point in an advanced intelligent network that receives narrowband signaling for a call originating at an end office for call processing and control within the advanced intelligent network; and

a centralized control and signaling interworking function (CS-IWF) device in an ATM switching network that receives the narrowband signaling from the signaling transfer point and converts the received narrowband signaling to broadband signaling for processing and controlling the call within the ATM switching network;

wherein the CS-IWF device provides the broadband signaling to a plurality of trunk interworking function (T-IWF) devices via the ATM switching network, for establishing a connection across the ATM switching network, only when the CS-IWF device and the plurality of T-IWF devices are determined to be members of a closed user group.

17. The secure ATM distributed virtual tandem switching system, according to claim 16, in which the narrowband signaling comprises common channel signaling.

18. The secure ATM distributed virtual tandem switching system, according to claim 17, in which the broadband signaling comprises in-band signaling.

19. The secure ATM distributed virtual tandem switching system, according to claim 18, in which the in-band signaling comprises a plurality of packets.

20. The secure ATM distributed virtual tandem switching system, according to claim 18, wherein the common channel signaling comprises Signaling System 7 (SS7) signaling, and the in-band signaling comprises one of Private Network-Network Interface (PNNI) and User-to-Network Interface (UNI) signaling.

21. The secure ATM distributed virtual tandem switching system, according to claim 16, further comprising:

an ATM element management system that receives and stores a list of network elements in the closed user group, including the CS-IWF device and the plurality of T-IWF devices, wherein determining that the CS-IWF device and the plurality of T-IWF devices are

members of the closed user group comprises using the ATM element management system list.

22. The secure ATM distributed virtual tandem switching system, according to claim 16, in which the CS-IWF device belongs to more than one closed user group.

23. The secure ATM distributed virtual tandem switching system, according to claim 16, in which the CS-IWF device serves a metropolitan area.

24. An Asynchronous Transfer Mode (ATM) distributed virtual tandem switching system comprising:

an originating end office that originates a telephone call and forwards appropriate common channel signaling, including at least one ISUP message for setting up a call, within an advanced intelligent network;

a signaling transfer point that receives and forwards common channel signaling for call processing and control within the advanced intelligent network;

a centralized control and signaling interworking function (CS-IWF) device that receives the common channel signaling from the signaling transfer point and converts the common channel signaling to broadband signaling to process and control the telephone call within an ATM switching network;

an originating trunk interworking function (T-IWF) device and a terminating T-IWF device that receive the broadband signaling from the CS-IWF device via the ATM switching network, the CS-IWF device and the T-IWF devices being in a closed user group; and

at least one ATM switch in the ATM switching network, the ATM switch establishing a connection for the telephone call across the ATM network, based on the broadband signaling, only when the CS-IWF device and the T-IWF devices are verified as being in the closed user group.

25. The secure ATM distributed virtual tandem switching system, according to claim 24, further comprising:

an ATM element management system that stores a list of network elements in the closed user group, including the CS-IWF device and the T-IWF devices, wherein the CS-IWF device and the T-IWF devices are verified as being in the closed user group based on the ATM element management system list.

26. The secure ATM distributed virtual tandem switching system, according to claim 25, in which the ATM switch verifies that an ATM End System Address (AESA) contained in calling party information in the broadband signaling from the CS-IWF device is consistent with a user-to-network interface between the originating T-IWF device and the ATM switch, the ATM switch not establishing the connection for the telephone call across the ATM network when the AESA is not consistent with the UNI.

27. The secure ATM distributed virtual tandem switching system, according to claim 26, in which the ATM switch sends an alarm to the ATM element management system when the AESA is not consistent with the UNI.